Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

A NEUROSECURITY PERSPECTIVE ON THE FORMATION OF INFORMATION SECURITY AWARENESS – PROPOSING A MULTI-METHOD APPROACH

Lennart Jaeger
German Graduate School of Management and Law, lennart.jaeger@ggs.de

Andreas Eckhardt
German Graduate School of Management and Law, andreas.eckhardt@ggs.de

A NEUROSECURITY PERSPECTIVE ON THE FORMATION OF INFORMATION SECURITY AWARENESS – PROPOSING A MULTI-METHOD APPROACH

Lennart Jaeger, Department of Human Resource Management, German Graduate School of Management and Law, Heilbronn, Germany, lennart.jaeger@ggs.de

Andreas Eckhardt, Department of Human Resource Management, German Graduate School of Management and Law, Heilbronn, Germany, andreas.eckhardt@ggs.de

Abstract

In today's digital age, in which all kinds of information can be accessed electronically at all times, organizations are under continuous pressure of keeping their information systems (IS) secure. To protect IS and information assets from insider threats, information security awareness (ISA) has been established as a crucial factor in influencing employees' behaviour that is supportive or disruptive of IS security. But yet to date, there is still a lack of in-depth and structured understanding of the factors influencing ISA. In this research-in-progress paper, we conduct a literature review to categorize determinants of ISA into four levels of origin (individual, organizational, social-environmental, and application-specific) and identify topics that are promising for future research. We then present our planned study as an example to pursue our recommendations. In the IS security context of phishing, we aim to uncover the extent to which non-IS professionals are able to develop an eye for technical aspects of IS security and pay higher visual attention to security and fraud indicators of web browsers and e-mails after being subject to different organizational awareness-raising activities. Among a survey and literature analysis, the multi-method approach uses the objective data collection instrument of eye tracking. We expect to contribute into the nascent area of neurosecurity research by offering new insights on the effectiveness of organizational means to increase employees' ISA.

Keywords: Information Security Awareness, Information Security, Eye tracking, Neurosecurity

1 INTRODUCTION

The "human factor" has become increasingly important for information systems (IS) security, since the end-user within organization is frequently seen as the weakest link in the appropriate protection of IS and information assets (Warkentin and Willison 2009). According to several research studies as well as industry reports, the vast majority of information security incidents and breaches result from intentional or unintentional actions ranging from detrimental misuse to human error committed by organizational insiders, i.e. employees with legal access to IS within an organization (Baker et al. 2010; Crossler et al. 2013; D'Arcy et al. 2009; Richardson 2011; Warkentin and Willison 2009). In respect thereof, information security awareness (ISA) has been established as a crucial determinant of successfully protecting IS from internal and external security threats and is regarded as an important indicator for the information security performance of an organization (Straub and Welke 1998; Tsohou et al. 2015). To increase the ISA among various organizational stakeholders and encourage security-related behaviour, organizations employ several non-technical security countermeasures such as information security policies and security education, training, and awareness (SETA) programs (D'Arcy et al. 2009). However, the success of these awareness-raising activities has not been without doubt in research and practice: many current SETA programs do not work as well as they could and employees have been found to ignore ISPs or purposely do the opposite of what they are supposed to do (Lowry et al. 2015; Tsohou et al. 2015).

Although the importance of ISA is widely recognized, knowledge about factors determining ISA remains limited despite calls for attention to this research gap by Bulgurcu et al. (2010) and subsequent efforts to contribute to close it (e.g. Haeussinger and Kranz 2013). To address this issue, we first conduct a literature review on proposed and/or empirically validated antecedents of ISA to provide a structured and fast access to the aggregated knowledge of the topic. More specifically, we aim to identify research gaps and depict areas in which additional studies are promising. Building on our recommendations, we present our planned study on phishing, which examines whether and to what extent non-IS professionals on different hierarchy levels scrutinize web browsers and e-mails visually for phishing attempts after being subject to organizational awareness-raising activities. Our multi-method approach uses, besides a survey, the NeuroIS method of eye tracking. In doing so, we echo recent calls to use such methods in order to better measure the complex interaction between information processing and decision making and gain further insights into the "black box" of user cognition (Anderson et al. 2016; Crossler et al. 2013). In our study, eye tracking is well suited to measure the effectiveness of awareness-raising activities, as it can fully capture participants' visual inspections of the characteristics of web-browsers and emails. In addition, we will be able to compare perceived (i.e. self-reported) levels of ISA with objective measures to assess actual levels of ISA. The remainder of the paper is structured as follows. First, we describe the methodology used for our literature review. Next, we analyse how literature defines ISA and then categorize antecedents of ISA into four levels of origin (individual, organizational, social-environmental, and application-specific). Based on our review, we discuss the findings critically and give implications for theory and practice. In addition, we point out gaps in previous research to uncover potential future research areas and work out recommendations using these insights. Based on our recommendations, we then offer insights into our planned study.

2 LITERATURE REVIEW

2.1 Methodology

The present literature review focuses on IS-related literature and to ensure a high quality of the literature base (Vom Brocke et al. 2009), peer-reviewed A+, A and B rated journals as well as conference proceedings of the IS sub-ranking of JOURQUAL 3 published by the German Academic Association for Business Research in 2015 were selected (see: http://vhbonline.org/en/service/jourqual/vhb-jourqual-3/teilrating-wi/). The 39 selected publication outlets were searched to determine whether a publication contained the term "awareness" in the title, abstract or keywords by using the search engine

provided and the following databases: ACM Digital Library, AISeL, EBSCOhost, IEEEXplore, ScienceDirect, and SpringerLink. We chose to use "awareness" as a broad search term, as the current body of knowledge is not consistent in terminologies on ISA. In doing so, a search result as comprehensive as possible was generated, i.e. 669 potentially relevant publications across 35 of 39 outlets were identified in total. Subsequently, the title, abstract, and full text of each publication was manually reviewed in detail to filter out those publications that did not primarily deal with awareness in research on IS security but were identified through the applied keyword search described above (e.g. if the term awareness was solely used to call attention to a certain issue in the paper). Using this filtering process, 21 articles were selected for the subsequent classification. One limitation in which deviate from the guidelines from vom Brocke et al. (2009) is that we did not perform a forward search. First, we take a closer look at how ISA is defined, since a coherent understanding of the concept is essential for valuable theoretical and practical investigations and implications (criterion 1). On top of this, the relationship of ISA with other constructs was investigated by several conceptual and empirical studies with rivalling research assumptions and paradigms. Thus, the second category focuses on potential influencing factors of ISA, i.e. the formation process of ISA (criterion 2). The third category of literature addresses aspects concerning outcomes of ISA, i.e. the consideration of ISA as an independent variable and other (most frequently behavioural) outcomes as dependent variables (criterion 3). However, for reasons of scope and our interest on determinants of ISA, the subsequent in-depth analysis focuses on criterion 1 and 2. The final set of 21 selected publications on awareness organized in alphabetical order of the authors along with their allocation to the three criteria of the classification scheme is presented in the following Table 1.

Author	1	2	3	Author	1	2	3	Author	1	2	3
Bulgurcu et al. (2010)	*	*	*	Haeussinger and Kranz (2013)	*	*	*	Rhee et al. (2005)	*		
Culnan et al. (2008)			*	Hovav and D'Arcy (2012)	*	*		Spears and Barki (2010)	*		*
D'Arcy et al. (2009)	*	*		Hu et al. (2007)			*	Straub and Welke (1998)		*	*
Dinev and Hu (2007)	*	*		Jenkins and Durcikova (2013)		*		Tsohou et al. (2015)	*		*
El-Haddadeh et al. (2012)	*			Ku et al. (2013)			*	Vance et al. (2013)		*	
Goodhue and Straub (1991)		*		Kumar et al. (2008)		*		Yayla (2011)		*	*
Hadasch et al. (2012)			*	Putri and Hovav (2014)		*		Zhang and Li (2015)	*	*	*

Note: 1=Definitions of awareness; 2=Outcomes of awareness; 3=Influencing factors of awareness.

Table 1. Correlation between publications and classification scheme (Criteria 1-3)

2.2 Definitions of Information Security Awareness

Despite some efforts to attenuate terminology ambiguity (e.g. Tsohou et al. 2008), a diffuse and partially inconsistent understanding of the term information security awareness (ISA) prevails, such as whether it refers to a product, a process, behaviour or even all three of them (Haeussinger and Kranz 2013) (see Table 2 for exemplary definitions on the three perspectives).

Aspect	Exemplary definition of information security awareness
Product	"In the current study, information security awareness (ISA) is defined as an employee's general **knowledge** about information security and his cognizance of the ISP of his organization." (Bulgurcu et al. 2010, p. 532)
Process	"Security awareness is a **process** that aims at changing individuals' perceptions, values, attitudes, behavior, norms, work habits, and organizational culture and structures with regard to secure information practices." (Tsohou et al. 2015, p. 1)
Behavior	"[…] In this sense, organizational awareness is conceptualized as a state that is reflected in the **behavior** of target groups." (Spears and Barki 2010, p. 515)

Table 2. Exemplary definitions on the three aspects of information security awareness

From a product perspective, ISA refers to an individual's cognitive state of mind in which individuals recognize the importance of IS security, are conscious about IS security objectives and pay attention towards IS security risks and threats. The definition by Bulgurcu et al. (2010) provides a very accurate representation of the product perspective of information security awareness (ISA), differentiating between an individual's knowledge and understanding of security issues as well as knowledge and understanding of information security policies. According to Rhee et al. (2005), information security

awareness does not only constitute an understanding of various information security threats, but also includes the perception of one's own vulnerability to said threats. Another approach to conceptualize ISA from the product perspective was taken by Zhang and Li (2015), who differentiate between perceived ISA and assessed ISA. Whereas the former refers to an individual's own perception about their ISA, the latter refers to their actual level assessed by a quiz test. The process perspective is based on the perception that ISA is not only a product in the form of a cognitive state of mind (i.e. knowledge or understanding applicable by the individual), but is described as the actual process of raising or maintaining awareness (i.e. the processes used to reach this state of mind). Tsohou et al. (2015) consider ISA as a process aiming to stimulate changes at several levels of an organization, in particular at the individual level (e.g. perception, value, attitude, behaviour, norm, work habits) as well as the organizational level (culture and structure). Similarly, El-Haddadeh et al. (2012) describe ISA as a continuous effort to raise attention and to induce a certain kind of behaviour. Some few definitions do not explain awareness solely as a state of mind, but also include aspects of actual behaviour. These actions relate to following technological issues (e.g. potential problems and solutions thereof) (Dinev and Hu 2007). Spears and Barki (2010) also follow partly the behavioural perspective by insinuating that organizational awareness of security risk management is a state expressed by the behaviour of several stakeholders within an organization.

2.3 Influencing Factors of Information Security Awareness

This section reviews publications proposing or empirically investigating influencing factors of ISA. The identified factors influencing ISA are organized according to their level of origin along four levels, namely individual, organizational, social-environmental, and application-specific (see Table 3). The first level includes factors originating from the employee or IS end-user and the second covers factors under the influence of the organization. The third level incorporates factors not under the direct influence of the organization's management but originating from an individual's interaction with his/her social environment, while the fourth covers factors originating from technical tools with integrated awareness-raising features that were designed and developed with the objective to increase awareness in specific software applications (e.g. web browser applications).

Influencing factors of information security awareness		**Author(s)**
Individual	Knowledge about IS	Haeussinger and Kranz (2013)
	Negative experience with IS security incidents	Bulgurcu et al. (2010); Haeussinger and Kranz (2013);
	Level of GPA	Zhang and Li (2015)
	Computer self-efficacy	Zhang and Li (2015)
Organizational	Formalization of work procedures	Hadasch et al. (2012)
	IS security communication	Hadasch et al. (2012)
	Management support of IS security initiatives	Hu et al. (2007)
	Perceived value of information	Hadasch et al. (2012)
	Provision and promotion of ISPs	Haeussinger and Kranz (2013)
	SETA program	Culnan et al. (2008); Haeussinger and Kranz (2013); Straub and Welke (1998); Tsohou et al. (2015); Yayla (2011); Zhang and Li (2015)
	User participation in security risk management	Spears and Barki (2010)
Social-environmental	Business partner IS security requirements	Hadasch et al. (2012)
	Secondary sources (media, news)	Haeussinger and Kranz (2013)
	Security-related behaviour of peers	Haeussinger and Kranz (2013)
	Public expectations of information protection	Hadasch et al. (2012)
	Regulatory requirements	Hadasch et al. (2012)
Application-specific	Just-in-time reminders; security warning messages	Jenkins and Durcikova (2013); Zhang and Li (2015)

Table 3. Influencing factors of information security awareness

With regard to influencing factors at the individual level, an individual's general knowledge about IS has been empirically found as a determinant of ISA, since the higher their knowledge of basic IS applications the more likely individuals are aware about security-related issues (Haeussinger and Kranz 2013). In addition, it is proposed by Bulgurcu et al. (2010) and empirically validated by Haeussinger and Kranz (2013) that the personal experience of information security incidents, such as a virus attack or punishment due to IS misuse behaviour, leads to a higher level of an individual's ISA. Furthermore, it was proposed but not yet empirically validated that a higher GPA reflecting learning motivation and ability, and computer self-efficacy implying being more familiar with computers, will increase an individual's ISA (Zhang and Li 2015).

With regard to influencing factors at the organizational level, it is suggested that the formalization of work procedures, which make it more likely that awareness-increasing security controls exist, IS security communication, and the individual's perception of value of information increases an individual's ISA through a heightened perception of importance of information protection (Hadasch et al. 2012). In addition, management's support of IS security initiatives by championing them is considered to be a main driver for making each individual aware of the importance of information security and evoking a company-wide ISA (Hu et al. 2007). Furthermore, information security policies (ISP) are considered to be an important information security management practice and the provision and promotion of IPS has been empirically found to be an effective organizational practice to increase individuals' awareness of information security issues (Haeussinger and Kranz 2013). Another important information security management practice to increase ISA of various stakeholders are so-called security education, training, and awareness (SETA) programs. They subsume the totality of various designs and measures related to the troika of security education, training, and awareness raising activities in an organization (Bulgurcu et al. 2010; Straub and Welke 1998). Empirical support for SETA programs increasing individuals' ISA has been provided by several studies (Culnan et al. 2008; D'Arcy et al. 2009; Haeussinger and Kranz 2013; Straub and Welke 1998). Another valuable method for raising ISA is the involvement of IS end-users in the development process of organizational information security controls. Spears and Barki (2010), for instance, applied user participation theories and empirically demonstrated that users' participation in the security risk management process contributed to an increased awareness of organizational policies, procedures and security risks along different target groups.

With regard to social-environmental factors affecting an individual's ISA, Hadasch et al. (2012) proposed that public expectations of information protection as well as security requirements from regulatory bodies and business partners heightens an individual's ISA through the individual's perception of information leakage incidents as being a threat. Last but not least, it has been empirically proven that observing security-related behaviour of colleagues (e.g. their ISP compliance) weakly influences an individual's ISA, whereas secondary sources (e.g. media information about security issues) have a stronger effect on ISA by awakening interest and knowledge about information security (Haeussinger and Kranz 2013).

Influencing factors at the application-dependent level originate from technical tools with integrated awareness features that were designed and developed with the objective to increase ISA in specific software applications by alerting the users to possible IS security threats that may arise. For instance, just-in-time reminders in the form of pop-ups as SETA program components intended to raise employees' ISA attract employees' attention and reminds them of what has been learned in previous security training about, for instance, disclosing customer information (Jenkins and Durcikova (2013). Similarly, the frequency of received information security warning messages was proposed but not yet empirically tested to increase individuals' levels of ISA (Zhang and Li 2015).

2.4 Identifying Research Topics for Influencing Factors of ISA

In this section, the findings of the literature review are critically discussed, implications for practice are given, research gaps are pointed out to uncover potential future research areas and recommendations are worked out using these insights.

Identifying and understanding the influencing factors of ISA yields crucial insights for practitioners (e.g. IS security managers) to ensure the success of information security objectives and encourage the desired security-related behaviour among employees. However, these determinants focus mainly on IS users' or employees' ISA, while the management perspective is largely left unregarded. Examining influencing factors of management's ISA is important in light of a study done by Taylor (2006) who identified an optimistic bias among managers, in particular managers were unaware of the security risk arising from employees' unintentional actions, perceived their company's security level to be high and assumed that employees adhere to security policies despite this not being the case. Therefore, a first direction for future research could be to investigate if different hierarchy levels (e.g. management and employee) depend on different influencing factors, i.e. whether the factors found to be influencing employees' ISA also influence managers' ISA. At the organizational level, SETA programs and ISPs have been identified as important security management practices to increase an individual's ISA. Although these practices intend to inform and educate employees and other end-users about security issues (e.g. security breaches and related risks), they also implicitly assume that a certain degree of knowledge is sufficient to allow them to develop the same level of ISA as, for instance, IS professionals. Yet, Vaast (2007) found by introducing a social representation perspective of IS security in the context of a healthcare organization that employees of different departments in the same organization differ in their perception of ISA, in particular what security actually involves. For instance, IS professionals focused on technical aspects of security, while other employees focused on the security of confidential data. They suggested that customized SETA programs, which take different stakeholders into account, are needed. Practitioners, such as security managers, should keep this in mind and customize their different security management practices (e.g. SETA programs, ISPs) to specific target groups instead of following a one-size-fits-all approach. Researchers could test which of these methods are most effective to raise the ISA of different stakeholders. It might be also fruitful to examine differences between employees' own perception of ISA, in particular how they self-rate their level of ISA, and actual level of ISA, i.e. objectively assessed ISA. Employees might think that their ISA is high but is actually low, and vice versa. Whereas these security management practices focus on non-technical means to increase an individual's ISA, future research should aim to explore further potential antecedents, which are for instance of technical nature. For this purpose, the effectiveness of tools providing information about security issues or referring to the organization's ISPs immediately before an IS security breach (e.g. an ISP violation) in raising an individual's ISA could be examined. This line of thought has been investigated in information privacy research (e.g. warning mechanisms provided by tools before disclosing personal information), but neglected to a large extent in IS security research on ISA.

In sum, we propose to consider different types of organizational stakeholders (IS professionals vs. non-IS professionals) or hierarchy levels (employees vs. management), differences between perceived and actual levels of ISA (i.e. use of subjective vs. objective data), and to compare the effectiveness of different technical and non-technical awareness-raising activities.

3 PLANNED STUDY

In the following, we propose our planned study as an example of how to address the topics discussed in section 2.4. Following the notion of Vaast (2007) that employees from different departments in an organization differ in their perception of ISA, we examine to what extent non-IS professionals on different hierarchy levels are able to develop an eye for technical aspects of IS security. In particular, we focus on features of web browsers and emails that convey authenticity or fraud, and examine whether non-IS professionals scrutinize web browsers and email messages more intensely after being subject to a security awareness program component (i.e. an online session on phishing) and warning messages on phishing sent by the organization's IT department. Phishing attacks are of concern for organizations and individuals alike, as they are often used to steal personal and organizational information assets and/or to spread viruses, worms, Trojan horses and malware (Herath et al. 2014).

The core idea is to utilize the analysis of eye tracking data (in particular eye fixation and eye movement patterns) in order to improve IS security. Eye tracking is a well-established method in cognitive psychology research and has been recently considered in the nascent area of neurosecurity research, which has gained increasing levels of support after recent calls to use NeuroIS methods to study IS security behaviour (Crossler et al. 2013). For instance, Anderson et al. (2016) use eye tracking to examine the occurrence of habituation when individuals repeatedly view security messages. Similarly research on phishing messages has made use of eye tracking to examine whether the assessment of a website's credibility can be extracted from eye movements (Miyamoto et al. 2014) and to explain users' susceptibility to phishing (Anderson et al. 2013). In line with this area of research we consider eyes to be suitable to monitor internal mental processes, as they provide objective information on whether individuals have the intention to look for something. It seems reasonable that employees who state that they have high levels of ISA also have the intention to visually check whether an e-mail or website is fraudulent. Combining eye tracking with survey methodology offers valuable insights into the extent to which employees' own perception of ISA (self-rating of their level of ISA) is congruent with their actual level of ISA, i.e. objectively assessed ISA. Moreover, eye tracking is well suited for measuring the effectiveness of the awareness-raising activities (in our case a session on phishing and warning messages), as it can fully capture participants' visual inspections of the characteristics of web-browsers and emails. Our goal is to provide answers to the following questions:

RQ1: Are employees with high levels of perceived ISA also more likely to look for indicators of security and fraud when using web browsers and emails at work?

RQ2: To what extent do employees give higher visual attention to these indicators after being subject to organizational awareness-raising activities?

3.1 Methodology

To address our research questions, our multi-method approach consists of an experiment using eye-tracker technology together with two surveys. We will conduct our study at a large financial institution in Germany and consider IS-professionals and non-IS professionals at this institution as our unit of analysis. We expect differences between those two groups based on recent research highlighting that phishing knowledge plays an important role in phishing detection as it strengthens the utilization of phishing deception indicators in decision making and reduces the impact of attention to visceral triggers (Wang et al. 2012). Our multi-method approach proceeds as follows. After being welcomed by the experimenter, the participant fills in a questionnaire in stage 1. In stage 2, the experimenter reads the task sheet, which includes a short note of the task to be fulfilled, out loud and hands it over to the participant to give him/her the opportunity to read the task again and to ask questions. In stage 3, the experimenter carries out the necessary preparations for the experiment such as calibrating the eye tracker. Next, the experiment starts with the task to be accomplished by the participant in stage 4. Upon completion of the experiment, the second survey is presented to the participant in stage 5.

3.1.1 Tasks and Treatment

We will implement a 2x2 factorial experiment, crossing a training session on phishing (present or missing) and warning messages (present or missing) resulting in four treatment conditions. The laboratory experiment will be designed to mimic a realistic scenario in which participants need to assess the urgency of an incoming email based on subject, text, URL link and attachment, and forward it to their supervisor in terms of their urgency. The set of emails will consist of authentic e-mails and real-world phishing examples in which attachment or URL links to websites are fraudulent and aim to fool individuals into submitting personal and/or organizational information. During this task, participants are randomly given a training session, warning messages, both, or neither. The treatments are intended to raise awareness about security threats related to phishing and inform participants about characteristics of web-browsers and e-mails that can serve as indicators of authenticity or fraud, which users may consider while assessing a website's or email's credibility such as a browser's SSL indicator, URL structure, email's sender address, among many others (Dhamija et al. 2006; Whalen and Inkpen 2005).

3.1.2 Data collection methods

In the IS context, two relevant types of gaze behaviour that are carried out for the purpose of detailed observation of visual or textual information and to refocus on additional target points can be differentiated: fixations and saccades (Rayner 1998); Eckhardt et al. 2012, 2013). Fixations are phases of relative stagnation of the eyes, in which stimulus areas taken into view (fixed) are seen through the fovea of the eyes. Saccades are very rapid eye movements that serve to align the eyes on a new visual target. Saccades and fixations alternate mutually in a continuous process. The initiation of a saccade can be bottom-up, i.e. triggered involuntarily and reflexively by sudden abnormal changes in the peripheral field of vision (e.g. by movements). On the other hand, saccades can also be initiated top-down, i.e. intentionally triggered by individuals to inspect peripherally perceived object that have attracted the attention of the viewer more accurately (Theeuwes 2010). There is a broad consensus that visual information can only be perceived and processed in fixations, whereas during saccades vision is limited extremely due to the rapid eye movements (Rayner 1998). In addition, we consider pupillometry (i.e. the measurement of changes in pupil diameter), which is controlled by the autonomic system and enables us to gage unconscious mental processes in addition to deliberate, conscious visual processing of visual stimuli (Buettner et al. 2015; Riedl et al. 2014). To collect ocular movements and in particular the gaze point of our participants on specific areas of interest (i.e. the characteristics of web-browsers and emails that convey credibility or fraud), we will use Tobii Pro X2-30 eye tracker, which is designed to capture data at 30 Hz and thus is well suited for research on gaze points. The eye tracker will be paired with and installed under a 19" LCD monitor, and tracks the participants' eyes during the entire experiment. In addition to collecting eye-tracking data that enables the objective assessment of actual levels of ISA among employees, we also consider subjective data to assess their perceived levels of ISA. Our survey consists of two chronologically separated parts. The first survey is administered before the experiment and takes into account the following elements: demographics, general and security-related IT knowledge and experience, and control variables in terms of the Big Five personality traits (McCrae and Costa 2003), which is a widel acknowledged, integrative taxonomy of most human individual differences categories that are important, meaningful, and consequential. After the experiment, we will administer a second survey, which includes measurements to capture the participants' perceived level of ISA (general ISA; Bulgurcu et al. 2010), attitudes towards behaviour and behavioural intentions (Fishbein and Ajzen 1975). A summary of the three stages of our multi-method experimental analysis is depicted in Table 5.

Stage	Pre-experimental Stage	Experimental Stage	Post-Experimental Stage
Data	Subjective	Objective	Subjective
	Demographics, personality, IT knowledge	Number and duration of fixations, number of saccades	ISA, attitudes, behavioural intentions
Data Collection	Pre-experimental survey	Eye-tracker	Post-experimental survey

Table 5. Experimental Design

3.2 Expected Contributions and Implications

This study is expected to contribute to the nascent area of NeuroIS security research, also termed neurosecurity, which is an umbrella term for IS security research applying methods and theories of neuroscience to obtain greater insights into the so-called "black box" of user cognition (Anderson et al. 2015). Whereas extant research on ISA has predominantly made use of self-reported measures (e.g. interview and survey data), these measures may be subject to social desirability bias, subjectivity bias, and common method bias (Anderson et al. 2016). NeuroIS tools such as eye tracking can help mitigating these challenges by objectively measuring awareness of IS security threats (e.g. phishing) as it occurs. Our study is also expected to provide meaningful implications for practitioners on how to sharpen their employees' eyes for IS security threats.

References

Anderson, B., Vance, A., & Eargle, D. (2013). Is Your Susceptibility to Phishing Dependent on Your Memory? In *Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy*. Paper 40.

Anderson, B. B., Kirwan, C. B., Eargle, D., Jensen, S. R., & Vance, A. (2015). Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: A neurosecurity study. *Journal of Cybersecurity, 1*(1), 109–120.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *European Journal of Information Systems* (23 February 2016).

Baker, W., Goudie, M., Hutton, A., Hylender, C., Niemantsverdriet, J., & Novak, C. (2010). Verizon 2010 data breach investigations report. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf. Accessed 18 May 2015.

Buettner, R., Sauer, S., Maier, C., & Eckhardt, A. (2015). Towards Ex Ante Prediction of User Performance: A Novel NeuroIS Methodology Based on Real-Time Measurement of Mental Effort. In *48th Hawaii International Conference 2015*, pp. 533–542.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security, 32*(1), 90–101.

Culnan, M. J., Foxman, E. R., & Ray, A. W. (2008). Why IT Executives Should Help Employees Secure Their Home Computers. *MIS Quarterly Executive, 7*(1), 49–56.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79–98.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems, 8*(2), 386–408.

Eckhardt, A., Maier, C., & Buettner, R. (2012). The Influence of pressure to perform and experience on changing perceptions and user performance: a multi-method experimental analysis. In *Proceedings of the 2012 International Conference on Information Systems (ICIS 2012)*. Orlando, Florida, USA.

Eckhardt, A., Maier, C., Hsieh, J. J., Chuk, T., Chan, A., Hsiao, J., & Buettner, R. (2013). Objective measures of IS usage behavior under conditions of experience and pressure using eye fixation data. In *Proceedings of the 2013 International Conference on Information Systems (ICIS 2013)*. Milan, Italy.

El-Haddadeh, R., Tsohou, A., & Karyda, M. (2012). Implementation Challenges for Information Security Awareness Initiatives in E-Government. In *Proceedings of the 20th European Conference on Information 2012, ECIS 2012*. Barcelona, Spain. Paper 179.

Fishbein, M., and Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*, Reading, MA: Addison-Wesley.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users. *Information & Management, 20*(1), 13–27.

Hadasch, F., Mueller, B., & Maedche, A. (2012). Exploring Antecedent Environmental and Organizational Factors to User-Caused Information Leaks: a Qualitative Study. In *20th European Conference on Information, ECIS 2012*. Barcelona, Spain. 127.

Haeussinger, F., & Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. In *Proceedings of the 34th International Conference on Information Systems (ICIS), Milan, Italy*. Paper 1149.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. (2014). "Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service," *Information Systems Journal* (24:1), pp. 61–84.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99–110.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153–172.

Jenkins, J. L., & Durcikova, A. (2013). What, I Shouldn't Have Done That?: The Influence of Training and Just-in-Time Reminders on Secure Behavior. In *Proceedings of the International Conference on Information Systems, ICIS 2013*. Milano, Italy, December 15-18, 2013. Paper 7.

Ku, Y.-C., Chen, R., & Zhang, H. (2013). Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan. *Information & Management, 50*(7), 571–581.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254–264.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193–273. doi:10.1111/isj.12063

McCrae, R. R., & Costa, P. T. (2003). *Personality in adulthood: A five-factor theory perspective* : Guilford Press.

Miyamoto, D., Iimura, T., Blanc, G., Tazaki, H., & Kadobayashi, Y. (2014). EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits. In *Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)* .

Putri, F. F., & Hovav, A. (2014). Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory. In *22nd European Conference on Information Systems, ECIS 2014*. Tel Aviv, Israel, June 9-11, 2014.

Rauthmann, J. F., Seubert, C. T., Sachse, P., & Furtner, M. R. (2012). Eyes as windows to the soul: Gazing behavior is related to personality. *Journal of Research in Personality, 46*(2), 147-156.

Rayner, K. (1998). Eye movements in reading and information processing: 20 years of research. *Psychological bulletin, 124*(3), 372.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. In *Proceedings of the International Conference on Information Systems, ICIS 2005,*. December 11-14, 2005, Las Vegas, NV, USA. Paper 32.

Riedl, R., Davis, F. D., & Hevner, A. R. (2014). Towards a NeuroIS research methodology: intensifying the discussion on methods, tools, and measurement. *Journal of the Association for Information Systems, 15*(10), I.

Richardson, R. (2011). 2010/2011 CSI computer crime and security survey. http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html. Accessed 18 June 2015.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441.

Taylor, R. (2006). Management Perception of Unintentional Information Security Risks. In (Paper 95).

Theeuwes, J. (2010). Top–down and bottom–up control of visual selection. *Acta psychologica, 135*(2), 77–99.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38–58.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective, 17*(5-6), 207–227. doi:10.1080/19393550802492487

Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. *The Journal of Strategic Information Systems, 16*(2), 130–152.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems, 29*(4), 263–290.

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009).
Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search
Process. In *17th European Conference on Information Systems, ECIS 2009*, Verona, Italy, pp. 2206-2217.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on,Professional Communication, 55*(4), 345-362.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101–105.

Whalen, T., & Inkpen, K. M. (2005). Gathering evidence: use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*. Canadian Human-Computer Communications Society.

Yayla, A. A. (2011). Controlling insider threats with information security policies. In *19th European Conference on Information Systems, ECIS 2011*. Helsinki, Finland, June 9-11 2011. Paper 242.

Zhang, P., & Li, X. (2015). Determinants of Information Security Awareness: An Empirical Investigation in Higher Education. In *Proceedings of the International Conference on Information Systems 2015*. Fort Worth, Texas.